

File Note Title: Genl Cor - denial letter

Create Date: 12/29/2014 9:18 AM

Author: MIKE MAILLET

File Note Text:

File Note Created By: Mike Maillet

Date File Note Created: 12/29/2014 9:18:11 AM

Date Email Sent: 12/24/2014 12:19:12 PM

Email Sent From: CN=Michael Maillet/O=ChubbMail

Email Sent To: Michael Otner <motner@mdsol.com>

Email Copied To: jgaudette@wgains.com, william.leone@nortonrosefulbright.com

Subject: Medidata-Crime Loss

Dear Mr. Otner:

Please see the attached copy of correspondence with reference to the above matter.

Michael Maillet

Senior Claim Examiner

Chubb & Son, a division of Federal Insurance Company

Specialty Claim Service Center, 82 Hopmeadow Street, Simsbury, CT 06070-7683

Phone: (212) 612-2484 | Fax: (855) 842-1349 | mmaillet@chubb.com



CHUBB GROUP OF INSURANCE COMPANIES

Specialty Claim Service Center
82 Hopmeadow Street
Simsbury, CT 06070-7683
Phone: (212) 612-4000

Direct Dial (212) 612-2484

December 24, 2014

Via email and first-class mail

Michael Otner, Esq.
General Counsel
Medidata Solutions, Inc.
350 Hudson Street
9th Floor
New York, NY 10014

Re: Company: Federal Insurance Company
 Insured: Medidata Solutions, Inc.
 Policy No.: 8212-1392
 Claim No.: 339763
 Matter: Medidata Solutions, Inc.-Crime Loss

Dear Mr. Otner:

This is a follow up to our telephone conference of December 4, 2014, in which we discussed the above-referenced claim by Medidata Solutions, Inc. ("Medidata") under the Crime Coverage Section of the Executive Protection Portfolio Policy (the "Policy"). Federal Insurance Company ("Federal") has now completed its review of the information provided by Medidata in support of the claim, and the terms and provisions of the Policy. Federal has determined that coverage is not afforded for this loss under the Crime Coverage Section of the Policy and respectfully denies coverage for the reasons set forth herein.

We understand that this matter involves a wire transfer of \$4,827,200 by Medidata to a bank account in Shanghai, on or about September 18, 2014. The wire transfer was initiated by a Medidata employee and was authorized by two other Medidata employees. These employees acted upon a series of fraudulent emails purporting to be from the [REDACTED] of Medidata, [REDACTED], and a purported attorney, Michael Meyer. The emails in the name of [REDACTED] were sent from an email address that appears to be identical to his actual email address, [REDACTED]. However, the reply-to address was secureop@dr.com. We were informed that once the emails entered Medidata's email platform, the email system automatically added details including a photograph of [REDACTED]. The emails from Michael Meyer were sent from mmever@consultant.com.

Medidata has advised us that its systems were not penetrated and that the emails purporting to be from [REDACTED] were spoofs, even though they used an address identical to his actual email address. We were informed during our December 4th telephone conference that there are third-party web sites that will allow emails to be created using a third-party's email address and a different reply-to address.

Federal wrote the Policy for the policy period of June 25, 2014 through June 25, 2015. The Crime Coverage Section of the Policy contains several insuring clauses, with each insuring clause providing a separate limit of liability and retention. We have reviewed each of the insuring clauses within the Crime Coverage Section and have determined that no insuring clause is triggered by the circumstances of this loss. We will, however, discuss the three insuring clauses mentioned during our telephone conference: *Forgery Coverage Insuring Clause 4*; *Computer Fraud Coverage Insuring Clause 5*, and *Funds Transfer Fraud Coverage Insuring Clause 6*. Each is subject to a \$5,000,000 limit and a \$50,000 retention.

Please refer to the following pertinent Insuring Clauses and Definitions contained within the Policy:

In consideration of payment of the premium and subject to the Declarations, the General Terms and Conditions, and the limitations, conditions, provisions and other terms of this coverage section, the Company and the Insureds agree as follows:

Forgery Coverage Insuring Clause 4

The Company shall pay the **Parent Organization** for direct loss sustained by an **Organization** resulting from **Forgery** or alteration of a **Financial Instrument** committed by a **Third Party**, including:

- (a) any check or draft made or drawn in the name of such **Organization** payable to a fictitious payee and endorsed in the name of such fictitious payee;
- (b) any check or draft procured in a face to face transaction with such **Organization** or with one acting as the agent of such **Organization** by a **Third Party** impersonating another and made or drawn payable to the one impersonated and endorsed by a **Third Party** other than such one impersonated; and
- (c) any payroll check, payroll draft or payroll order made or drawn by such **Organization** payable to bearer as well as to a named payee and endorsed by a **Third Party** other than such named payee without the authority of such named payee.

Computer Fraud Coverage Insuring Clause 5

The Company shall pay the **Parent Organization** for direct loss of **Money**, **Securities** or **Property** sustained by an **Organization** resulting from **Computer Fraud** committed by a **Third Party**.

Funds Transfer Fraud Coverage Insuring Clause 6

The Company shall pay the **Parent Organization** for direct loss of **Money** or **Securities** sustained by an **Organization** resulting from **Funds Transfer Fraud** committed by a **Third Party**.

Definitions

11. When used in this coverage section:

Computer Fraud means the unlawful taking or the fraudulently induced transfer of **Money**, **Securities** or **Property** resulting from a **Computer Violation**.

Computer Violation means the fraudulent:

- (a) entry of **Data** into or deletion of **Data** from a **Computer System**;
- (b) change to **Data** elements or program logic of a **Computer System**, which is kept in machine readable format; or
- (c) introduction of instructions, programmatic or otherwise, which propagate themselves through a **Computer System**,

directed against an **Organization**.

Computer System means a computer and all input, output, processing, storage, off-line media library and communication facilities which are connected to such computer, provided that such computer and facilities are:

- (a) owned and operated by an **Organization**;
- (b) leased and operated by an **Organization**; or
- (c) utilized by an **Organization**.

Financial Instrument means a check, draft or similar written promise, order or direction to pay a sum certain in **Money** that is made, drawn by or drawn upon an **Organization** or made or drawn by anyone acting as an **Organization's** agent, or that is purported to have been so made or drawn.

Forgery means the signing of the name of another natural person or organization, with the intent to deceive, but does not mean a signature that includes, in whole or in part, one's own name, with or without authority, in any capacity for any purpose. Mechanically or electronically produced or reproduced signatures shall be treated the same as hand-written signatures.

Funds Transfer Fraud means fraudulent electronic, telegraphic, cable, teletype, facsimile, telephone or written instructions (other than **Forgery**), purportedly issued by an **Organization**, and issued to a financial institution directing such institution to transfer, pay or deliver **Money** or **Securities** from any account maintained by such **Organization** at such institution, without such **Organization's** knowledge or consent.

Forgery Coverage Insuring Clause 4:

The term **Forgery** is defined to require "the signing of the name of another natural person or organization." In addition, the Forgery Coverage applies only if there is a **Forgery** or alteration on a **Financial Instrument**, as that term is defined. The emails in this claim did not contain any signature, but even if they did, the insuring clause requires that the **Forgery** be on a **Financial Instrument**. The emails are not a **Financial Instrument**, as that term is defined. They are not similar to checks or drafts, drawn by or upon Medidata, but simply purported to be internal communications requesting that Medidata employees issue instructions to Medidata's bank. Therefore, we cannot agree that an e-mail qualifies as a **Financial Instrument**, as required by Insuring Clause 4.

In addition, Insuring Clause 4 requires that the loss result directly from the **Forgery**. Even if there was a **Forgery** in this instance, which we do not believe to be the case, the alleged **Forgery** on an e-mail did not result in any direct loss to Medidata. If Medidata employees had not acted on the e-mails and had not instructed payment to be made Medidata's bank, there would have been no loss. In fact, there was at least one prior incident in which a similar spoofed email did not result in any loss. Therefore, Medidata did not sustain a direct loss resulting from any **Forgery** on an e-mail.

Computer Fraud Coverage Insuring Clause 5:

In order for Computer Fraud Coverage to apply, there must be a direct loss of **Money, Securities or Property** sustained by an Insured resulting from **Computer Fraud** committed by a **Third Party**. The definition of **Computer Fraud** requires an unlawful taking or fraudulently induced transfer of **Money, Securities or Property** resulting from a **Computer Violation**. For the reasons stated herein, the circumstances as described by Medidata do not fall within any of the three sub-paragraphs of the definition of **Computer Violation**.

In order for there to be a **Computer Violation** under Section (a) of the definition, there must be a "fraudulent entry of **Data** into or deletion of **Data** from a **Computer System** . . . directed against an **Organization**." In this matter, there was no fraudulent entry of **Data** into Medidata's **Computer System**. The subject emails containing false information were sent to an inbox which was open to receive emails from any member of the public. While the content of the emails was fictitious, the entry of those emails into the **Computer System** was authorized. Similarly, there is no evidence of any fraudulent deletion of **Data** from the **Computer System**. Therefore, Section (a) of the definition of **Computer Violation** has not been met.

In order for Section (b) of the definition of **Computer Violation** to apply, there must be a "fraudulent change to **Data** elements or program logic of a **Computer System**, which is kept in machine readable format . . . directed against an **Organization**." In this case, we are not aware of any facts suggesting that the emails caused any fraudulent change to **Data** elements or program logic of Medidata's **Computer System**. In our telephone conference on December 4, 2014, there was a discussion about how Medidata's email system populated the emails purporting to be from [REDACTED] with additional data, such as a picture of [REDACTED]. While this may be the case, the email did not fraudulently cause this to happen. It was Medidata's

Computer System that populated the email, in the normal manner. In addition, it has not been suggested that there was any change in the **Data** elements that were applied to the emails. Therefore Section (b) of the definition of **Computer Violation** does not apply.

In order for Section (c) of the definition of **Computer Violation** to apply, there must be a "fraudulent introduction of instructions, programmatic or otherwise, which propagate themselves through a **Computer System** . . . directed against an **Organization**." In this case, there was no fraudulent introduction of the emails. As noted previously, any member of the public was authorized to send emails to Medidata's email system. In addition, the emails did not contain instructions that propagated themselves through Medidata's **Computer System**. They were simply emails that had no power to propagate themselves. Thus, Section (c) of the definition of **Computer Violation** does not apply.

In addition, for the same reasons discussed with respect to the Forgery Coverage insuring clause, Medidata's loss does not constitute a direct loss as required under the Computer Fraud Coverage insuring clause.

Because this matter does not fall within any of the components of the definition of **Computer Violation**, and because the loss was not a direct loss resulting from **Computer Fraud**, there is no coverage available under the Computer Fraud Coverage insuring clause.

Funds Transfer Fraud Coverage Insuring Clause 6:

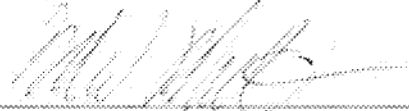
Under the definition of **Funds Transfer Fraud**, there must be a fraudulent instruction purportedly issued by Medidata to a financial institution directing a transfer of funds, without Medidata's knowledge or consent. In this case, the fraudulent emails do not fit within this definition because, among other reasons, they were sent to Medidata, not to a financial institution. The wire instructions sent to Medidata's bank also do not fit within the definition. Medidata itself, and not an entity purporting to be Medidata, sent the wire request to its financial institution. Furthermore, since Medidata itself issued the wire instructions to its bank, the **Money** was wired with Medidata's knowledge and consent. Thus, there is no coverage available under the Funds Transfer Fraud Coverage insuring clause.

Based on the above, we respectfully deny coverage for this loss under *Insuring Clauses 4, 5 and 6* of the Crime Coverage Section of the Policy. Pursuant to our review of the Crime Coverage Section of the Policy, we cannot identify any other relevant insuring clauses that may apply. If you would like us to review this claim under another insuring clause, please identify the insuring clause under which you believe coverage applies and why. We would be happy to conduct a further analysis.

This letter is not intended to waive any rights or defenses of Federal Insurance Company, which it may now have and which may hereafter accrue by reason of the terms and conditions of the above captioned policy of insurance, or otherwise. All of Federal Insurance Company's rights and defenses are specifically reserved. If you have any questions regarding this matter, please feel free to contact me.

Very truly yours

Chubb & Son
A division of Federal Insurance Company
Manager



Michael A. Maillet, Esq.
New York Specialty Claims

cc.: via email

James W. Gaudette, Esq.
Vice President & Executive Risk Claims Counsel
William Gallagher Associates
470 Atlantic Avenue
Boston, MA 02210

Bill Leone, Esq., Partner
Fulbright & Jaworski LLP
666 Fifth Avenue
New York, New York 10103-3198